Department of Homeland Security Daily Open Source Infrastructure Report for 13 June 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports Social Security numbers and other personal data for 12,000 Georgia employees was accessible for weeks on a government Website, and the state only learned of the breach when a former employee reported it. (See item 5)
- The Department of Homeland Security announced on Friday, June 9, the release of two Federal regulations to help businesses comply with current legal hiring requirements intended to reduce the employment of unauthorized aliens. (See item 21)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 11, New York Times* — **Russia bargains for bigger stake in West's energy.** Russian, American, European and Japanese officials are negotiating over whether Russia should be allowed greater latitude to invest in utilities, pipelines, natural gas facilities and other infrastructure in the United States and Europe. In a draft declaration for endorsement at a Group of 8 summit meeting next month in St. Petersburg, Russia, broadened Russian access is paired with something the West wants: endorsement of market principles and greater access for foreign investment in the energy industry of Russia, one of the biggest oil and natural gas producers in the world. Russian investment in U.S. energy facilities has been relatively modest,

like Lukoil's investment in a chain of 2,000 filling stations in the United States. Now the Russians appear interested in investing in pipelines and liquefied natural gas conversion facilities on the East Coast. The United States is looking to the meeting to endorse President Bush's vision of "energy security," particularly reduced dependence on Middle East oil, greater variety of oil resources and more nuclear power. One other important part of the American vision is that there should be more efforts to bypass Russia for natural gas exports, especially to Europe.
Source: http://www.nytimes.com/2006/06/12/world/europe/12russia.html

2. *June 11, Associated Press* — **World feels China's growing thirst for oil.** Chinese demand for oil is forecast to more than double by 2025, to 14.2 million barrels a day from the current 7 million a day, according to the U.S. government's Energy Information Agency. Although China's imports still only constitute about one−sixth of total world oil trade, it is already the world's second largest oil consumer. China's increasingly pivotal role as global manufacturer of practically everything has ensured demand will continue to grow. "Oil — the dependence upon oil is a national security problem, and an economic security problem," President Bush said recently. The worry in Washington, Tokyo and other major oil importing centers is that competition is helping push prices to potentially destabilizing levels, and raising the risks of conflict over dwindling resources. China has sought to diversify its energy sources, clinching exploration and production deals in Africa and Latin America to limit its dependence on Middle Eastern oil. China still gets more than two−thirds of its energy from coal, and roughly half of its oil supply is from domestic sources−−3.4 million barrels a day in 2005. But veteran fields are beginning to falter and motor vehicle use is surging.
Source: http://www.msnbc.msn.com/id/13169547/

3. *June 09, MarketWatch* — **Energy sector recasts storm survival plans.** Hurricane season opened June 1 amid dire predictions by the National Oceanic and Atmospheric Administration that the Atlantic and Gulf Coasts face an 80 percent chance of above−normal hurricane activity. Government officials called a news conference this spring at which they cautioned that it would take just two back−to−back storms like Katrina and Rita to wreck substantial havoc on the sector, halt the flow of some energy supplies and trigger a new spike in gasoline prices. This year, oil companies are stockpiling emergency supplies in other parts of the country, working with local and federal officials, the Red Cross and U.S. Coast Guard to better coordinate their response efforts. But the widespread devastation following Katrina scuttled some industry efforts to restore operations. In several cases, local or federal authorities confiscated pumps and generators for emergency medical purposes, delaying the reopening of major pipelines carrying fuel from Gulf Coast refineries to Midwest and Northeast markets. Companies may be able to do little to prevent the same thing from happening again, according to the National Petrochemical & Refiners Association, which notified its members that Louisiana law grants a parish president authority to commandeer supplies in a disaster.
Source: http://www.marketwatch.com/News/Story/Story.aspx?guid=%7b6158127A−AABF−41D3−976E−25E3C17F28C3%7d&siteId=google

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *June 12, Courier Post Online (NJ)* — **Diesel spill blamed for highway closure.** Traffic was closed late Saturday, June 10, and early Sunday, June 11, on Route 130 in Burlington Township, NJ, because of a diesel spill on the road. A 2000 Freightliner tractor trailer owned by the Jevic Trucking Co. was crossing Route 130 from a jughandle when it struck the center concrete median, causing fuel tanks to leak diesel onto the road.
Source: http://www.courierpostonline.com/apps/pbcs.dll/article?AID=/20060612/NEWS01/60612002

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *June 12, Associated Press* — **Personal data on thousands of Georgia state workers posted online.** Social Security numbers and other personal data for 12,000 Georgia employees was accessible for weeks on a government Website, and the state only learned of the breach when a former employee reported it. Because of a coding error, the data for thousands of active state workers in an employee recognition program was inadvertently made available to anyone searching the agency's Website, Deborah Williams, a spokesperson for the Georgia Merit System said. The affected employees will receive a letter in the mail from the Georgia Merit System, the state's personnel agency. Williams said no fraud has been reported by any of the workers whose data was made public. Anyone with additional questions about the incident should call 404−651−6300
Source: http://www.ledger−enquirer.com/mld/ledgerenquirer/14800789.h tm

6. *June 12, Government Accountability Office* — **GAO−06−483: International Financial Crime: Treasury's Roles and Responsibilities Relating to Selected Provisions of the USA PATRIOT Act (Report).** Money laundering and terrorist financing can severely affect the nation's economy and also result in loss of lives. To combat these transnational crimes, the Treasury Department (Treasury) and its component bureau, the Financial Crimes Enforcement Network (FinCEN), have key roles. Section 330 of the USA PATRIOT Act encourages the federal government to engage foreign jurisdictions in negotiations to ensure that foreign banks and financial institutions maintain adequate records to combat international financial crime. Treasury plays a lead role in facilitating such efforts. In accordance with its various responsibilities codified by section 361, FinCEN is to coordinate with its foreign counterparts−−financial intelligence units (FIU). This report describes (1) Treasury's approach for negotiating with foreign jurisdictions, (2) how FinCEN has contributed to establishing FIUs in foreign countries and enhancing the capabilities of these units, and (3) what actions FinCEN is taking to maximize its performance as a global partner.
Highlights: http://www.gao.gov/highlights/d06483high.pdf
Source: http://www.gao.gov/new.items/d06483.pdf

7. *June 11, Newsday* — **A final fraud leads to longer sentence.** Identity thief Kevin Walker, 42, of Brooklyn, NY, was given a 96−month term in federal prison last week for bank fraud, a sentence that was increased by two years after he allegedly tried to fake his death to avoid being sentenced. Federal investigators told Brooklyn federal Judge John Gleeson that Walker, who stole more than $210,000 through various identity−theft schemes, falsely claimed he was terminally ill with cancer at a local hospice. Although Walker later denied it, officials believe that to avoid being sentenced, he tried to assume the identity of a gravely ill man with the same name, who later died. Walker was convicted in October of bank fraud. He originally was arrested in February 2005 on a criminal complaint accusing him of emptying the bank account of a North Carolina woman who had died in 1997. The complaint also accused Walker of depositing a counterfeit check in a Brooklyn bank account held in the dead woman's name.
Source: http://seattletimes.nwsource.com/html/nationworld/2003053980_fraud11.html

8. *June 11, Associated Press* — **China's Bank of Communications reports fraud case.** Bank of Communications Co., China's fifth largest bank by assets, has reported a fraud case it said involved 200 million yuan ($24.9 million) at a branch in the northeastern city of Shenyang. The Hong Kong−listed bank said in a statement on its Website over the weekend that it was working with security authorities to investigate the case. The case was the third admission of fraud at Chinese banks in the past week. Banking analysts have said that risk management and corporate governance at Chinese banks are still just being put in place and that the banks face a significant risk of more bad loans building up.
Source: http://www.chron.com/disp/story.mpl/ap/fn/3960925.html

9. *June 09, Business First of Louisville (KY)* — **Former bank manager pleads guilty to fraud.** Carol C. Ezell, a former bank manager with Bank One (now Chase) in Louisville, KY, has pled guilty to bank fraud According to a news release from the David Huber, U.S. Attorney for the Western District of Kentucky, Ezell, 38, admitted that between April 1, 1999, and March 13, 2001, she approved falsely collateralized loans, misapplied loan proceeds, authorized fraudulent loans, authorized impermissible overdraws of lines of credit, and embezzled bank funds for her own use, resulting in a loss of more than $925,000. Ezell is scheduled to be sentenced on September 7, in Louisville.
Source: http://www.bizjournals.com/louisville/stories/2006/06/05/dai ly31.html

[Return to top]

Transportation and Border Security Sector

10. *June 12, Reuters* — **U.S. airlines can find capital for right deal.** A Bush administration plan to ease restrictions on foreign investment in U.S. airlines could help a struggling industry, but analysts and consultants say there is plenty of money at home for the right deal. "The airline industry is awash in capital," said Darryl Jenkins, an industry consultant who also is a visiting professor at Embry−Riddle Aeronautical University. Jenkins and others point to last year's merger between US Airways Group Inc. and America West Airlines Inc. as evidence the industry does not require foreign capital to move forward. Much of the $870 million raised for that deal came from hedge funds, domestic airlines, and other sources. Industry observers also agree U.S.−based investors were ready to participate in the reorganization of UAL Corp.'s United Airlines before the carrier financed its bankruptcy exit with debt. Robert Mann, an

airline industry consultant in Port Washington, NY, also notes investors are "shoving and elbowing" to get in line for any potential merger involving bankrupt carriers Northwest Airlines Corp. and Delta Air Lines Inc. whether they combine or strike separate deals.
Source: http://www.usatoday.com/travel/flights/2006−06−12−us−airline −capital_x.htm

11. *June 12, Associated Press* — **Bag prompts Florida airport shutdown, evacuation.** A food writer's bag containing recording equipment, honey, an oyster shell, and seasoning rub was blamed for three−hour shutdown and evacuation of the Tallahassee's airport Monday, June 12, authorities said. The configuration of the electronic gear and organic material looked suspicious when Transportation Security Administration officers scanned the carryon luggage, said Tallahassee police officer David McCranie. Todd Coleman, food editor for New York−based Saveur magazine, was detained but later released after the bag was removed from the terminal and a robot opened it to disclose the contents.
Source: http://wireservice.wired.com/wired/story.asp?section=Breakin g&storyId=1535608

12. *June 09, Government Accountability Office* — **GAO−06−630: Airline Deregulation: Reregulating the Airline Industry Would Likely Reverse Consumer Benefits and Not Save Airline Pensions (Report).** The Airline Deregulation Act of 1978 phased out the government's control over fares and service and allowed market forces to determine the price and level of domestic airline service in the United States. The intent was to increase competition and thereby lead to lower fares and improved service. In 2005, the Government Accountability Office (GAO) reported on the tenuous finances of some airlines that have led to bankruptcy and pension terminations, in particular among those airlines that predated deregulation (referred to as legacy airlines). The House Report accompanying the 2006 Department of Transportation (DOT) Appropriation Act expressed concern about airline pension defaults and charged GAO with analyzing the impact of re−regulating the airline industry on reducing potential pension defaults by airlines. GAO subsequently agreed to address the pension issue within a broad assessment of the airline industry since deregulation. Specifically, GAO is reporting on, among other things, (1) broad airline industry changes since deregulation, (2) fare and service changes since deregulation, and (3) whether there is evidence that re−regulation of entry and fares would benefit consumers or the airline industry, or save airline pensions. DOT agreed with the conclusions in this report. GAO is making no recommendations in this report.
Highlights: http://www.gao.gov/highlights/d06630high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−630

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *June 12, Advertiser (Australia)* — **Mystery disease at sugarcane farm.** A Queensland, Australia, farm has been quarantined following the discovery of a mystery disease in a

sugarcane crop. The Department of Primary Industries and Fisheries and sugar industry body BSES Ltd are trying to determine the exact nature of the disease found in the mature plantation in Childers. A spokesperson said the priority was to ensure the disease did not spread and affect other sugarcane properties in the Childers district.
Source: http://www.theadvertiser.news.com.au/common/story_page/0,5936,19443284%255E1702,00.html

14. *June 11, Associated Press* — **Sudden oak death contained on southern Oregon coast.** Sudden oak death −− a threat to Oregon's $800 million nursery crop industry −− has been contained on the southern Oregon coast, agriculture officials say. But the project to eradicate the plant fungus has produced mixed results. A five−year multi−agency effort to completely get rid of the tree−killing disease has not yet reached its goal, but officials say they are encouraged it hasn't spread far beyond its original detection site northeast of Brookings. The site has included less than 88 acres of infected plant material, and remains the only place in Oregon where the fungus −− Phytophthora ramorum −− has been found in the natural environment. The fungus left a trail of dead trees in central and Northern California ever since it was first detected in the San Francisco Bay Area in the mid−1990s. Sudden oak death infects susceptible trees through the bark, killing the entire tree or portions of it. Certain species of oak commonly found in southwest Oregon, including tanoak and black oak, are very susceptible. But the fungus also infects rhododendron, huckleberry, madrone, myrtle, and several other shrubs.
Sudden oak death information: http://www.aphis.usda.gov/ppq/ispm/pramorum/
Source: http://www.kgw.com/sharedcontent/APStories/stories/D8I689EG0 .html

15. *June 09, Stop Soybean Rust News* — **Florida soybean rust is back on kudzu, not traveling yet.** Asian soybean rust is active again on kudzu in Gadsden, FL, even through the state is still quite dry. Officials think several nights of dew may have been enough for germination. Jim Marois, University of Florida professor of plant pathology, reported Friday, June 9, that: "We are having local showers, but overall the state is still very dry. Yesterday, June 8, we once again found soybean rust on kudzu in Gadsden County. This is the site in the panhandle of Florida that was positive in January, then negative during February after freezing weather, positive again in March when it warmed up, then negative again in April and May when we got dry. What is interesting is that the severity was moderate −− a lot of leaves had several lesions. This may mean the rust, since we have had little rain, is getting its water for germination from dew −− which we have had overnight for several days. The Florida kudzu canopy is fully developed, and flowering has begun in several areas. All of the soybean sentinel plots are still negative."
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=843

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

16. *June 11, Los Angeles Times* — **Water quest shifts course.** A powerful thirst is building in Southern California as forecasters predict the addition of about two million new households in the region over the next 20 years. In the past, finding water for all those extra showers, toilets and lawn sprinklers would have been easy: Look beyond a mountain range, find a wild river and divert it to Los Angeles. But those days are over. The rivers are tapped, and there's more competition for their resources. Water customers across the region −− including vineyards, housing subdivisions, parks, restaurants and farms −− are in the midst of an ambitious push to find more efficient ways to use water. Southern California today gets half of its water from imported sources, compared with two−thirds a decade ago. Per capita water use in the region was 205 gallons a day 10 years ago; today it's about 175 gallons. Doing more with less has become the cornerstone of water management policy for one of the biggest and driest megalopolises on the continent. Unlike previous droughts, the last one −− which ran from 1999 to 2003 and required no rationing in Southern California −− went largely unnoticed because of the success of such programs, officials said.
Source: http://www.latimes.com/news/printedition/california/la−me−water11jun11,1,5235181.story?coll=la−headlines−pe−california

[Return to top]

Public Health Sector

17. *June 12, Independent (United Kingdom)* — **Bangladesh immunizes millions against polio.** More than half a million health workers and volunteers fanned out across Bangladesh on Sunday, June 11, to immunize up to 24 million children under the age of five in a United Nations backed campaign to eradicate polio from the country. The workers administered the vaccine to children at about 120 000 centers across the country in the final stage of a three−phase program for a polio−free Bangladesh. The campaign was launched after a nine−year−old child was recently paralyzed by the P1 polio virus in the eastern district of Chandpur, in what is believed to be Bangladesh's first case since August 2000. It was not clear how the child was infected, but the same virus has been found in parts of neighboring India. More than 20−million children under the age of five were vaccinated in the first two immunization rounds on April 16 and May 13.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.iol.co.za/index.php?set_id=14&click_id=117&art_id=qw1150063021135B215

18. *June 11, New York Times* — **Concern grows over increase in diabetes around world.** The number of people around the world suffering from diabetes has skyrocketed in the last two decades, from 30 million to 230 million, claiming millions of lives and severely taxing the ability of health care systems to deal with the epidemic. While the growing problem of diabetes in the affluent U.S. has been well documented, seven of the 10 countries with the highest number of diabetics are in the developing world. China now has the largest number of diabetics over age 20, around 39 million people. India has the second largest number of cases with an estimated 30 million people. In some countries in the Caribbean and the Middle East, the percentage of diabetic people range from 12 to 20 percent. “Diabetes is one of the biggest health catastrophes the world has ever seen,” said Martin Silink, the president−elect of the International Diabetes Federation. “The diabetes epidemic will overwhelm health care

resources everywhere if governments do not take action."
Source: http://www.nytimes.com/2006/06/11/health/11diabetes.html?_r= 1&oref=slogin

19. *June 10, ABC News (Australia)* — **China moves to contain bird flu outbreak.** China has culled about 17,000 poultry to contain an outbreak of bird flu in the country's northwest. China's latest outbreak of H5N1 bird flu was found on a farm in the northwestern province of Xinjiang. The country's official newsagency says the outbreak has been contained after a series of swift measures. About 17,000 poultry were killed, and experts and veterinarians killed birds and disinfected the area to prevent possible new outbreaks.
Source: http://www.abc.net.au/news/newsitems/200606/s1660075.htm

[Return to top]

Government Sector

20. *June 10, Washington Post* — **DC area's security proposal scored poorly.** The Department of Homeland Security sharply cut the Washington region's anti−terrorism funding in part because its grant application was among the weakest nationwide −− with one proposal scoring so low that money cannot be drawn without federal permission, officials said. The region's spending proposals were less innovative and less likely to produce sustained, high−impact results than those submitted by other cities, DHS officials said. The application ranked in the bottom 25 percent of those submitted by urban areas from across the country. George W. Foresman, DHS undersecretary for preparedness, said the region's ranking indicates that its proposals were less likely to produce tangible, sustainable improvements than some other applicants' ideas. The Washington region still got the fourth−highest grant−−$46 million, behind New York, Los Angeles and Chicago. But local officials had expected an increase from the $77 million they received last year. One reason it is difficult to justify more money for the capital region is that it already has federal forces helping to protect it, including the military, Foresman said. Also, the area has already received hundreds of millions of dollars in DHS anti−terrorism money in recent years, he said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/09/AR2006060901769.html

21. *June 09, Department of Homeland Security* — **DHS announces Federal regulations to improve worksite enforcement and asks Congress to approve Social Security "no match" data sharing.** The Department of Homeland Security (DHS) announced Friday, June 9, the release of two Federal regulations to help businesses comply with current legal hiring requirements intended to reduce the employment of unauthorized aliens. The first proposal would permit U.S. businesses to digitize their I−9 employment forms, which are used to verify eligibility to work in the United States. The other proposed regulation would set forth guidance for U.S. businesses when handling no−match letters from the Social Security Administration (SSA) concerning submitted employee Social Security numbers or from DHS concerning documents submitted by employees during the I−9 process. These proposed regulations are now subject to a 60−day public comment period, although the I−9 regulation will become effective on an interim basis as soon as it is published. As Congress continues to consider comprehensive immigration reform, DHS continues to urge them to increase the authority of the SSA to share information about Social Security "no match" letters with DHS worksite

enforcement agents. This information would allow DHS to learn which employers had received "no match" letters from SSA. It also assists investigators in identifying companies with the highest rate of immigration fraud.
Source: http://www.dhs.gov/dhspublic/display?content=5684

[Return to top]

Emergency Services Sector

22. *June 09, Air Force Print News* — **U.S. Air Force bracing for the storm.** In 2005, four major hurricanes −− Dennis, Katrina, Rita and Wilma −− combined to produce more than $1 billion in damage to Air Force installations, and commanders are doing everything in their power to ensure their units are ready should they face another storm. This year, Airmen at every coastal base from Florida to Louisiana have conducted base−wide hurricane preparedness exercises that ready the population's ability to respond in short notice if a storm is bearing down on them. Most base commanders also have published hurricane readiness articles and supplements in their base newspapers. "We know from Hurricane Katrina last year and countless other storms that preparedness is the key to withstanding these ferocious forces of nature," said General Paul Capasso, 81st Training Wing commander at Keesler Air Force Base, MS. "As well prepared as we've been at Keesler in the past, we're determined to do even better this year." While Keesler received the biggest blow from Hurricane Katrina during last year's record−setting season, five other installations in Florida also received varying levels of damage from Hurricanes Dennis, Katrina and Wilma.
Source: http://www.af.mil/news/story.asp?storyID=123021478

[Return to top]

Information Technology and Telecommunications Sector

23. *June 12, eWeek* — **Microsoft: Trojans, bots are significant and tangible threat.** Microsoft security researchers have used data collected from its malicious software removal tool (MSRT) to produce the clearest picture yet of the malware scourge on Windows. The software maker offered a rare glimpse of the extent of infected Windows systems, warning that the threat from backdoor Trojans and bots present "a significant and tangible threat." It is the first public confirmation by Microsoft that well−organized mobsters have established control of a global billion−dollar crime network using keystroke loggers, IRC bots and rootkits. Since the first iteration of the MSRT in January 2005, Microsoft has removed 16 million instances of malicious software from 5.7 million unique Windows machines. The most significant threat is clearly from backdoor Trojans, small programs that open a back door to allow a remote attacker to have unauthorized access to the compromised computer. The MSRT has removed at least one Trojan from about 3.5 million unique computers. Of the 5.7 million infected Windows machines, about 62 percent was found with a Trojan or bot.
Source: http://www.eweek.com/article2/0,1895,1974620,00.asp

24. *June 09, IDG News* — **U.S. House defeats net neutrality provision.** The U.S. House of Representatives has defeated a provision to require U.S. broadband providers to offer the same

speed of service to competitors that's available to partners, a major defeat to a coalition of online companies and consumer groups. The vote against the net neutrality amendment late Thursday, June 8 came after a last−minute push for the measure from many technology companies. After the House defeated the net neutrality amendment, it passed the underlying bill, a wide−ranging broadband bill focused partly on speeding the roll−out of television over Internet Protocol (IPTV). The underlying broadband bill, the Communications Opportunity, Promotion, and Enhancement Act, passed by a vote of 321−101 and will allow the U.S. Federal Communications Commission to investigate complaints about broadband providers blocking or impairing Internet content only after the fact. The bill also streamlines local franchising requirements for telecom carriers that want to offer IPTV services in competition with cable television. The bill in essence creates a national franchise, allowing AT&T and Verizon to roll out their IPTV services without going through lengthy franchising negotiations with each local government where they want to provide service.
Source: http://www.infoworld.com/article/06/06/09/79138_HNnetneutral itydefeat_1.html

25. *June 09, CNET News* — **Microsoft to ease up on piracy check−ins.** Microsoft plans to update the Windows Genuine Advantage (WGA) Notifications program so that it only checks in with Microsoft once every two weeks, instead of after each boot−up. By year's end, the tool will stop pinging Microsoft altogether. The changes come after critics likened the antipiracy tool to spyware because the program, designed to validate whether a copy of Windows has been legitimately acquired, checks in with Microsoft on a daily basis. "We are changing this feature to only check for a new settings file every 14 days," Microsoft said in a statement on its Website. "Also, this feature will be disabled when WGA Notifications launches worldwide later this year."
Microsoft's statement: http://www.microsoft.com/presspass/features/2006/jun06/06−08 wgaqa.mspx
Source: http://news.zdnet.com/2100−1009_22−6082334.html?tag=zdfd.new sfeed

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow:
http://www.kb.cert.org/vuls/id/4049100

Symantec Advisory SYM06−010 − Symantec Client Security and Symantec AntiVirus Elevation of Privilege:

http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. More information about the reported vulnerability can be found in the following:

TRA06−139A − Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.htmll

VU#446012 − Microsoft Word buffer overflow:
http://www.kb.cert.org/vuls/id/446012

Review the workarounds described in Microsoft Security Advisory 919637:
http://www.microsoft.com/technet/security/advisory/919637.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 50497 (−−−), 24232 (−−−), 25 (smtp), 80 (www), 32788 (−−−), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

26. *June 11, Boston Globe* — **Most schools don't check bus driver histories.** A survey by Globe North has found that most local school systems rely on outside transportation companies to conduct criminal history checks on the drivers they employ −− and several acknowledge that they do not review the results. The practice violates state law, which prohibits school officials from relying on background checks conducted by another entity, and is raising concerns in the aftermath of an investigation that found a convicted sex offender working for a Braintree, MA, bus company. Twenty−nine of the 35 public school districts in the Globe North circulation area rely on private bus, van, or taxi companies to transport some or all of their students to class. Six districts use only school employees to transport students. And, although all the districts conduct background checks on their own drivers, only a handful of school systems request Criminal Offender Record Information, or CORI, data from the state Criminal History Systems Board on their contractor s' drivers. Twenty−five of the 29 don't bother, either because school administrators mistakenly believed that privacy laws prohibit them from obtaining the data or because they misinterpreted the state's CORI statute and thought it was acceptable to have an outside party conduct the checks on their behalf.
Source: http://www.boston.com/news/local/articles/2006/06/11/most_schools_dont_check_bus_driver_histories/

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer